Política de Seguridad de la Información

24/07/2024

ISOTÁDER

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
Política de Seguridad ISOTADER CALIDAD	1.0	Primera versión	24-07-2024

CLASIFICACIÓN

USO INTERNO
La información contenida en este documento es USO INTERNO. Es responsabilidad del Área o Departamento receptor de este documento su distribución interna en base a la necesidad de conocer la información aquí contenida.

CONTROL DE DIFUSIÓN

AUTOR/ES: MIÓLNIR CYBERSEC S.L.
DISTRIBUCIÓN: ISOTADER CALIDAD S.L.

Tabla de contenido

1. Introducción

1.1 Introducción

La presente Política de Seguridad de la Información proporciona las bases para definir y delimitar los objetivos y responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran para garantizar la seguridad de la información, cumpliendo el marco legal de aplicación y las directivas, políticas específicas y procedimientos definidos.

Estas actuaciones son seleccionadas e implantadas en base a un análisis de riesgos realizado y el equilibrio entre riesgo aceptable y coste de las medidas.

El Responsable de Seguridad debe definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de la actividad realizada, de modo que los procesos más importantes y/o sensibles recibirán mayor protección.

Es responsabilidad del Comité de Seguridad de la Información (CSI), promover y apoyar la implantación de las medidas técnicas y organizativas necesarias para minimizar los riesgos potenciales a los que se encuentra expuesta la información en la consecución de los objetivos estratégicos del negocio.

El objeto de esta Política es alcanzar una protección adecuada de la información de la Compañía, preservando los siguientes principios de la seguridad:

- **Confidencialidad:** garantizar que la información sea accesible sólo para quien esté autorizado a tener acceso a la misma.
- **Integridad:** garantizar la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad:** garantizar que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Estos principios básicos se deben preservar y asegurar en cualquiera de las formas que adopte la información, ya sea en formato electrónico, impreso, visual o hablado, e independientemente de que sea tratada en las dependencias de la Compañía o fuera de ellas.

Asimismo, estos principios se deberán contemplar en las siguientes áreas de seguridad:

- **Física:** Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información.
- **Lógica:** Incluyendo los aspectos de protección de aplicaciones, redes y prototipos de comunicación electrónica y sistemas informáticos.
- **Político-corporativa:** Formada por los aspectos de seguridad relativos a la propia Compañía, a las normas internas, regulaciones y normativa legal.

1.2 Objetivos

La norma UNE-EN-ISO 27001:2023 es un estándar de seguridad internacional para Sistemas de Gestión de Seguridad de la Información que proporciona requisitos obligatorios para implementar, revisar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI).

Esta Política de Seguridad de las TIC (en adelante, Política) define y engloba la política del SGSI en términos de las características del Negocio, la Compañía y sus Activos.

Esta Política establece los principios, ambiciones y objetivos de la Compañía al utilizar el Sistema de Gestión para la Seguridad de la Información para cumplir los mismos.

1.3 Alcance

La presente Política es aplicable a todos los activos de información incluyendo instalaciones, sistemas, servicios, software, bases de datos y toda la información almacenada o procesada en los sistemas informáticos.

Asimismo, deberán cumplir con la Política de Seguridad todas las personas que tengan acceso a la información objeto de alcance del Sistema de Gestión de Seguridad de la Información, y/o presten servicios para la Compañía, incluso en el supuesto de que su relación no tenga carácter laboral.

2. La organización

2.1 Misión

La misión que se persigue es la que se describe a continuación:

- Ser el equipo estratégico de nuestros clientes para alcanzar la excelencia, aunando experiencia en nuevas tecnologías y capital humano.
- Aportar soluciones en toda la cadena de valor.
- Desarrollar un sistema integral de optimización de las relaciones de nuestros clientes con su mercado.

2.2 Visión

- Mejorar cada día nuestro servicio 360 de gestión de la experiencia con el cliente.
- Consolidar nuestro liderazgo en el sector de experiencias con el cliente

2.3 Valores

- Compromiso
- Honestidad
- Sostenibilidad
- Calidad
- Competitividad
- Constancia

- Transparencia
- Cercanía
- Fidelidad
- Pasión
- Innovación
- Trabajo en equipo
- Ética

3. Marco normativo

La normativa a la que se encuentra sometida la Compañía, más relacionada con su actividad, se recoge a continuación.

- Código Penal (Ley Orgánica 10/1995, de 23 de Noviembre)
  1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
     - Artículo 197. Se tipifican en este artículo las conductas que llevan a apoderarse de mensajes de correo electrónico ajenos o acceden a documentos privados sin la autorización de sus titulares.
     - Artículos 264.2 y 278.3. Hacen referencia a la destrucción, alteración o daño de programas o documentos contenidos en ordenadores.
     - Artículo 278.1. Se refiere a apoderarse o difundir documentos o datos electrónicos de empresas.
  2. Delitos informáticos.
     - Artículo 248.2 Este artículo se refiere a las estafas como consecuencia de alguna manipulación informática.
     - Artículo 256. Hace referencia a la utilización no consentida de un ordenador sin la autorización de su dueño causándole un perjuicio económico superior a 300,50€
  3. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.
     - Artículo 270. Tipifica la copia no autorizada de programas de ordenador así como la fabricación, distribución o tenencia de programas que vulneran las medidas de protección anti-piratería de los programas.
  4. Ataques que se producen contra el derecho a la intimidad.
     - Artículos del 197 al 201. Se refieren a delitos de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos
  5. Falsedades.
     - Artículos 386 y siguientes. Hacen referencia al concepto de documento como todo soporte material que exprese e incorpore datos y a la fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad.
  6. Sabotajes informáticos.

    - Artículos 263 y otros. Hablan del delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos
  7. Fraudes informáticos.
    - Artículos 248 y siguientes. Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos, RGPD).
- LOPDGDD (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

4. Política de Seguridad

Esta Política de Seguridad de la información ha sido desarrollada para asegurar la confidencialidad, integridad y disponibilidad de la tecnología y los activos de información de la Compañía (p.e. aplicaciones de IT, sistemas y servicios) y se alinea con el estándar UNE-EN-ISO 27001:2023 “Tecnologías de la Información – Técnicas de Seguridad – Código de prácticas para los controles de seguridad de la información”. Asimismo, esta Política hace referencia a la Normativa General de Seguridad de la Información.

5. Objetivos generales de seguridad

El SGSI tiene como objetivo principal asegurar la confidencialidad, disponibilidad e integridad de los sistemas de información que dan soporte a los procesos, sistemas e infraestructura de la Compañía, según el documento de aplicabilidad. Para ello, tiene como objetivos concretos:

- Proteger, mediante controles/medidas, los activos frente a amenazas que puedan derivar en incidentes de seguridad.
- Paliar los efectos de los incidentes de seguridad.
- Establecer un sistema de clasificación de la información y los datos con el fin de proteger los activos críticos de información.
- Definir las responsabilidades en materia de seguridad de la información generando la estructura organizativa correspondiente.

- Elaborar un conjunto de reglas, estándares y procedimientos aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- Especificar los efectos que conlleva el incumplimiento de la Política de Seguridad en el ámbito laboral.
- Evaluar los riesgos que afectan a los activos, con el objeto de adoptar las medidas/controles de seguridad oportunos.
- Verificar el funcionamiento de las medidas/controles de seguridad mediante auditorías de seguridad internas realizadas por auditores independientes.
- Formar a los usuarios en la gestión de la seguridad y en tecnologías de la información y las comunicaciones.
- Proteger a las personas en caso de catástrofes naturales, incendios, inundaciones, ataques terroristas, etc., mediante planes de emergencia.
- Controlar el tráfico de información y de datos a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- Observar y cumplir la legislación en materia de protección de datos, propiedad intelectual, laboral, penal, etc., que afecte a los activos de la Compañía.
- Garantizar un servicio eficiente a nuestros clientes con un alto nivel de calidad, preservando así su confianza.
- Proteger el capital intelectual de la Compañía para que no se divulgue ni se utilice ilícitamente.
- Obtener las evidencias que permitan acreditar los incidentes de seguridad y la identificación de su autor.
- Reducir las posibilidades de indisponibilidad a través del uso adecuado de los activos de la Compañía.
- Defender los activos ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- Controlar el funcionamiento de las medidas de seguridad averiguando el número de incidencias, su naturaleza y efectos.

Las distintas áreas cuya responsabilidad se encuentran bajo los servicios prestados deberán contemplar la seguridad desde el mismo momento en que se concibe un nuevo sistema o servicio, aplicando para estos y para los ya existentes, las medidas de seguridad necesarias para garantizar la disponibilidad, confidencialidad e integridad de la información.

Los requisitos de seguridad de los sistemas, las necesidades de formación de los usuarios, administradores y operadores y las necesidades de financiación deben ser identificados e incluidos en la planificación de los sistemas y en los pliegos de prescripciones utilizados para la realización de proyectos que involucren a las TIC.

Se deben articular mecanismos de prevención, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.

En cuanto a la prevención, se debe evitar que los servicios y la información resulten afectados por un incidente de seguridad. Para ello, la Compañía implementará las medidas

de seguridad que les son de aplicación en base a las normativas y regulaciones (referenciadas en el apartado 3 de Marco Normativo) que afectan a su actividad, así como las medidas adicionales necesarias para contrarrestar las amenazas identificadas en el proceso de análisis de riesgos.

En cuanto a la reacción, se establecerán mecanismos de detección, comunicación y gestión de incidentes de seguridad, de forma que cualquier incidente pueda ser tratado en el menor plazo posible. Siempre que sea posible, se detectarán de forma automática los incidentes de seguridad, utilizando elementos de monitorización de los servicios o de detección de anomalías y poniendo en marcha los procedimientos de respuesta al incidente en el menor plazo posible. Para los incidentes detectados por los usuarios, ya sean internos o externos, se establecerán los pertinentes canales de comunicación de incidentes.

En cuanto a la recuperación, para aquellos servicios que se consideren críticos, en base a la valoración que de los mismos realicen sus responsables, se deberán desarrollar planes que permitan la continuidad de los mismos en el caso de que, a raíz de un incidente de seguridad, quedaran indisponibles.

6. Organización de la Seguridad

Una correcta organización de la seguridad, constituye la base necesaria para mantener la seguridad de los sistemas de información y establece los roles y responsabilidades necesarios para proteger los activos de información, garantizando la integridad, disponibilidad y confidencialidad de los mismos, cumpliendo con el marco legal vigente y respetando las directrices, normas y procedimientos que oportunamente se establezcan.

La asignación de responsabilidades y funciones respecto a la seguridad de la información es parte de las responsabilidades de la Dirección y una base fundamental para la implementación de un Sistema de Gestión de la Seguridad de la Información basado en la Norma UNE-EN-ISO 27001:2023.

La seguridad en la Compañía está soportada sobre las estructuras y roles que se describen a continuación:

- Estructura de especificación, que es la que se encarga de establecer los requisitos de seguridad asociados a los servicios y productos prestados.
- Estructura de supervisión, que es la que se encarga de verificar el cumplimiento de los requisitos de seguridad y el alineamiento continuo con los objetivos de la Compañía.
- Estructura de operación, que se encarga de implantar las medidas de seguridad identificadas.

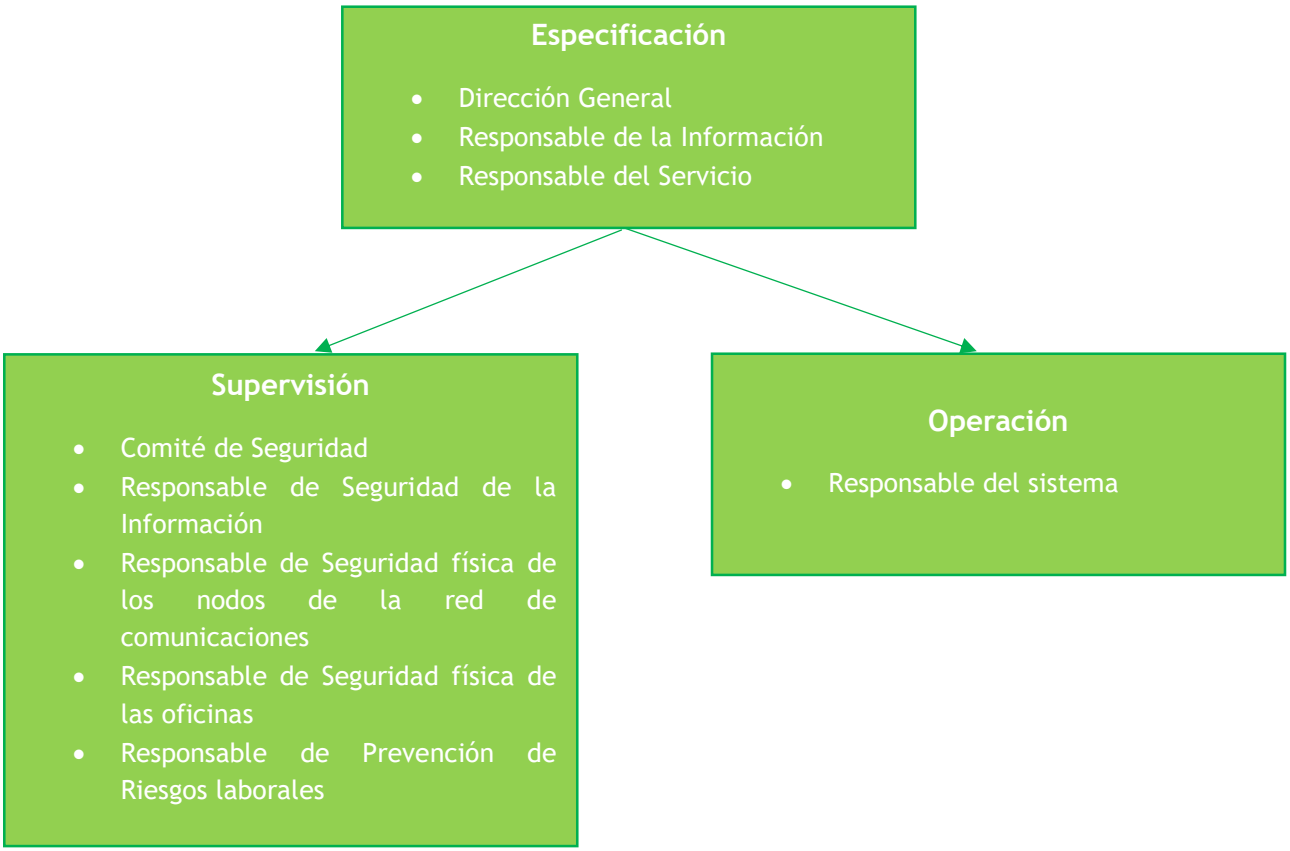

Ilustración 1 – Responsabilidades en materia de Seguridad

6.1 Estructura de especificación

Esta estructura es la encargada de determinar los requisitos de seguridad que serán de aplicación a los servicios prestados por la Compañía y a garantizar el cumplimiento normativo asociado que le es de aplicación y la norma ISO 27001.

Forman parte de esta estructura:

- El Responsable de la Información.
- El Responsable del Servicio.
- Comité de Dirección.

Las figuras de Responsable de la Información y del Servicio establecerán el nivel de seguridad que la información y los servicios prestados por la Compañía requieren, en base a sus exigencias en cuanto a disponibilidad, confidencialidad e integridad, considerando el impacto que tendría en el Negocio y en los clientes la falta de alguno de esos aspectos.

6.1.1 Responsable de la Información y Responsable del Servicio (RIS)
Estos roles pueden recaer en personas diferentes o en la misma. Pueden existir varios responsables de la información y varios responsables de los servicios.

Sus funciones y responsabilidades son:

- Asignar el nivel de clasificación de los activos de información de los que sean responsables.
- Reclasificar los activos de información de los que sean responsables cuando sea necesario.
- Autorizar el acceso del personal de la compañía que tuviera la necesidad de conocer la información de la que fueran responsables.
- Apoyar en la concienciación en el uso correcto de los activos de información.
- Poner en conocimiento del Responsable de Seguridad de la Información cualquier incumplimiento de la normativa interna en materia de Seguridad de la Información.
- Participar en el seguimiento y resolución de aquellos incidentes de seguridad que afecten a la información que trata.

6.2 Estructura de supervisión

La estructura de supervisión de la seguridad se encarga de verificar la correcta implantación y operación de los requisitos de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.

En la supervisión global de todas las actividades relativas a la seguridad de la información se encuentra el Responsable de Seguridad de la Información.

Para la coordinación global e integral de la seguridad se encuentra el CSI.

Las funciones y responsabilidades de cada una de las figuras se describen a continuación.

6.2.1 Comité de Seguridad de la Información (CSI)

6.2.1.1 Composición del CSI

El CSI, depende del Comité de Dirección de la Compañía.

Para la celebración de las reuniones del CSI será preciso la presencia de, al menos, el 51% de los miembros permanentes.

Cualquier miembro permanente podrá delegar su asistencia a otra persona de la Compañía, siempre que esta acción quede formalmente documentada. De manera adicional, y según se requiera y acuerde por los miembros permanentes indicados anteriormente, podrán participar otros miembros con carácter temporal, de acuerdo a los temas que se traten por el CSI.

6.2.1.2 Objetivos y funciones

El CSI tiene como objetivos:

- Favorecer la creación, implantación, operación, supervisión, revisión, mantenimiento y mejora de la gestión de la seguridad.
- Asegurarse de que el personal esté formado para el desempeño de las responsabilidades que le han sido asignadas en lo concerniente al mantenimiento de la seguridad.
- Concienciar al personal afectado de la trascendencia y de la importancia de las actividades de seguridad de la información y de su contribución a los objetivos de seguridad.
- Proveer y gestionar los recursos necesarios para crear, implementar, operar, supervisar, revisar, mantener y mejorar la gestión de la seguridad.

Las funciones y responsabilidades asignadas a este comité son las siguientes:

- Velar por el establecimiento de los objetivos de seguridad y los planes para alcanzarlos. Ello conlleva, aprobar los documentos principales en los que se basa el SGSI.
- Comunicar a la Compañía la importancia de cumplir los objetivos y la política de seguridad de la información, sus responsabilidades legales y la necesidad de la mejora continua.
- Velar por que se realicen las auditorías internas de seguridad.
- Realizar el seguimiento de las revisiones del Sistema de Gestión de la Seguridad.
- Velar que los procedimientos de seguridad de la información responden a los requisitos empresariales.
- Ser conscientes y velar por el cumplimiento de los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
- Llevar a cabo revisiones, cuando sean necesarias, y reaccionar en base a los resultados de estas revisiones.
- Participar en la mejora de la eficacia del Sistema de Gestión de la Seguridad.
- Valorar la eficacia de las acciones realizadas.
- Ser partícipes de la eficacia de las acciones realizadas, para tomar decisiones adecuadas.
- Verificar la existencia de registros de educación, formación, aptitudes, experiencia y cualificaciones.

6.2.1.3 Reuniones del CSI

Las reuniones del CSI se realizarán con una periodicidad trimestral, con un mínimo de cuatro reuniones al año, aunque cualquier miembro permanente de dicho comité puede convocar reuniones extraordinarias cuando lo considere necesario, bien sea como respuesta a incidentes, cambios organizativos, como a cualquier otro aspecto que pueda afectar a la seguridad y sea de carácter urgente.

El contenido de las reuniones será el que se requiera para el cumplimiento de las funciones del CSI.

Con posterioridad a las reuniones, el Responsable de Seguridad de la Información, o la persona en la que éste delegue, generarán las pertinentes actas, en las cuales se recogerá, como mínimo, evidencia de los asuntos tratados y los acuerdos alcanzados, formando parte así de los registros del Sistema de Gestión de la Seguridad.

6.2.2 Responsable de Seguridad de la Información (RSEG)

- Objetivos y funciones:
- Formular la Política de Seguridad.
- Aprobar las Políticas de Seguridad de la Información.
- Aprobar el modelo de Clasificación y Gestión de Activos de Información.
- Asistir al personal en materia de Seguridad de la Información.
- Lanzar y participar hasta su cierre en las revisiones del SGSI por la dirección.
- Lanzar, participar y revisar los resultados de las auditorías internas y externas del SGSI (certificación o seguimiento del SGSI).
- Revisar aquellos documentos de los que sea el responsable y gestionar los procesos de revisión y aprobación de los documentos del SGSI, así como su carga en la plataforma documental del SGSI.
- Incluir en la agenda de reunión del CSI cualquier tema que le sea escalado en relación con el SGSI. En concreto se identifican los dos siguientes:
    - Gestión de recursos para el SGSI.
    - Revisión de la eficacia del SGSI.
    - Oportunidades de mejora como resultado de la aplicación de la política de seguridad y de los objetivos de seguridad.
    - Identificar a la persona/entidad externa encargada de realizarla auditoría interna del SGSI.
- Lanzar, participar y revisar los resultados de la actualización del análisis de riesgos, el plan de acción y el documento de aplicabilidad.
- Actualizar el inventario de activos en función de la información recibida por parte de administradores de sistemas, desarrolladores y personal implicado en el SGSI.
- Actualizar aquellos indicadores de los que es responsable y controlar que el resto de responsables actualizan los que tengan asignados.
- Lanzar, participar y revisar los resultados de las acciones propuestas como resultados de las auditorías internas y externas y revisiones por la dirección.
- Lanzar, participar y revisar los resultados de los proyectos del plan de acción.
- Lanzar, participar y revisar los resultados de los cursos de formación en materia de SGSI.
- Analizar, junto con los responsables de la información, los riesgos derivados del acceso a la información de la compañía.
- Verificar la aplicación de las medidas de seguridad necesarias para la protección de la Información.
- Definir el Modelo de Clasificación y la Gestión de Activos de la Información de la compañía.
- Definir y gestionar el Modelo de Organización y Gestión de la Seguridad del SGSI.

- Elaborar las políticas de seguridad de la información.
- Convocar las reuniones del CSI.
- Proponer los planes de gestión de riesgo y supervisar su implantación.
- Gestionar las No conformidades, Acciones Correctivas y Acciones Preventivas.
- Mantener actualizado el Análisis de Riesgos y el seguimiento del Plan de Tratamiento de Riesgos.
- Realizar las revisiones de seguridad.
- Elaborar los registros de seguridad.
- Evaluar la eficacia de las acciones realizadas e informar al CSI, para que se tome las medidas oportunas.
- Identificar y hacer cumplir los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.

6.2.3 Responsable de Prevención de Riesgos Laborales
Es responsable de la prevención de riesgos laborales de las oficinas y de los nodos de red de comunicaciones de la Compañía.

Sus responsabilidades comprenden:

- Controlar de las medidas de prevención de riesgos laborales del personal que accede a los nodos de la red de comunicaciones de ISOTADER CALIDAD SL y a las oficinas de la Compañía.
- Implantar medidas de seguridad para la protección frente a incendios.
- Implantar medidas de seguridad para la protección frente a inundaciones.
- Participar en el CSI.

ISOTADER CALIDAD SL dispone de la figura del responsable técnico de prevención dentro de la Estructura de operación.

La estructura de operación de la seguridad debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas necesarias para satisfacer los requisitos de seguridad establecidos por la estructura de especificación.

Se describen a continuación las funciones y responsabilidades de las figuras asociadas a la estructura de operación.

6.3 Estructura de operación

6.2.4 Responsable del Sistema (RSIS)
Sus funciones y responsabilidades son:

Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de los Sistemas de Información de la Compañía.

Garantizar que en el diseño de sistemas de información y redes de comunicaciones se contemplen desde el principio los aspectos necesarios de seguridad de la información en cuanto a disponibilidad, integridad, confidencialidad, autenticación, control de acceso, auditoría y registro.

Revisar que la configuración de seguridad tras la instalación de un sistema nuevo es la adecuada (perfil inicial de seguridad. Bastionado).

Revisar que la configuración de seguridad tras los cambios en un sistema sigue siendo la adecuada.

Seguir los foros de vulnerabilidades y elaboración del calendario de aplicación de parches para los sistemas de información, en función de los que surjan y el impacto que tengan en la seguridad (los parches mismos los aplicarán los administradores de sistemas).

Implantar las medidas de seguridad que resulten de los planes de tratamiento de riesgos o planes de acciones correctivas a raíz de las auditorías de seguridad de la información.

Mantener la seguridad adecuada mediante la aplicación correcta de todos los controles implantados.

Proporcionar datos para la alimentación de indicadores de seguridad de la información.

Supervisar los procedimientos de copia de seguridad.

Realizar auditorías técnicas periódicas de la infraestructura, sistemas y aplicaciones.

Verificar el funcionamiento de mecanismos de Control de Acceso que eviten que un usuario acceda a datos o recursos con derechos distintos de los autorizados, sin que en ningún caso se puedan desactivar.

Supervisar que por parte del CEEIM, el Control el acceso a los CPD previene los accesos físicos no autorizados del personal que accede a las áreas de los diferentes CPDs.

Supervisar que por parte del CEEIM, se asegura el suministro eléctrico para todo el equipamiento de NOC, equipamiento de los empleados de las oficinas, y de los servidores ubicados en el CPD.

Supervisar que por parte del CEEIM, el Control el acondicionamiento del CPD (temperatura y humedad).

Supervisar que por parte del CEEIM, se Protege del cableado de las oficinas y del CPD (protección frente a interferencias, cables ubicados en bandejas, etc.) de la Compañía.

6.4 Cambios de asignación de responsabilidades

Corresponde al CSI la aprobación de los cambios en las responsabilidades asignadas. Este comité elevará su decisión a la Dirección de la organización para su firma y comunicación dentro de la empresa.

7. Funciones y obligaciones

Al margen de las funciones y atribuciones que atañen al personal que integra el esquema organizativo responsable de la seguridad, se establecen a continuación las obligaciones del personal de la Compañía, así como de aquellos terceros que tengan acceso a sus sistemas de información.

7.1 Funciones y obligaciones del personal

Todo el personal de la Compañía que tenga algún tipo de relación con el uso, la gestión, mantenimiento y explotación de la información y de los servicios prestados sobre ella, tiene la obligación de conocer la Política de Seguridad y cumplirla. El CSI dispondrá los medios para que esta Política llegue a los afectados.

El personal afectado deberá asistir a una sesión de concienciación en materia de seguridad, al menos, una vez cada dos años. Se establecerá un plan de concienciación para impartir dichas sesiones.

Las personas con responsabilidad en el uso, la gestión, mantenimiento o explotación de los servicios soportados en las TIC recibirán formación para el manejo seguro de los sistemas, en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El personal tendrá como responsabilidades:

- Cumplir con las medidas establecidas en las políticas y procedimientos relativos a la seguridad de la información y comprender las consecuencias de su incumplimiento.
- Tratar la información de la compañía sólo para el desarrollo de sus funciones.
- Comunicar sin dilaciones aquellos incidentes de seguridad o malos usos de los activos de información de que tenga conocimiento.

7.2 Funciones y obligaciones de terceras partes

Las terceras partes que estén relacionadas con la gestión, mantenimiento o explotación de los servicios prestados por la Compañía serán hechos partícipes de esta Política. Las terceras partes quedarán obligadas al cumplimiento de esta Política y a las políticas o normativas que se puedan derivar de ella.

Las terceras partes podrán desarrollar sus propios procedimientos operativos para satisfacer la Política.

Se deberán establecer procedimientos específicos de comunicación de incidencias para que los terceros afectados puedan reportarlas.

El personal de las Terceras Partes deberá recibir sesiones de concienciación, tal como se exige para el personal propio.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte, el Responsable de Seguridad deberá realizar un informe del riesgo en que se incurre. Ese riesgo deberá ser aceptado por el CSI.

8. Formación y concienciación

Con carácter anual se realizará una acción de formación y concienciación en materia de seguridad.

El objetivo de la acción formativa y de concienciación es doble:

- mantener informado al personal más directamente relacionado con el manejo de información y los sistemas que la tratan sobre los procedimientos existentes de seguridad, riesgos, medidas de protección, planes de protección, etc.
- concienciar al personal, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

El primer objetivo se asocia a Formación y el segundo a Concienciación.

Las áreas responsables determinarán el formato de la acción de Formación y Concienciación, así como sus contenidos.

9. Gestión de riesgos

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.

Como metodología base para la realización de los análisis de riesgos se utilizará MAGERIT, siendo esta metodología la más recomendable para el sector público nacional.

El análisis se realizará:

- Regularmente, una vez al año.
- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- Cuando ocurra un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

De acuerdo con la escala de riesgos de la metodología MAGERIT, el nivel de riesgo deberá situarse por debajo de nivel MEDIO para considerarse de forma automática como aceptable (el riesgo residual máximo debe ser BAJO). Valores de riesgo residual mayores a BAJO deberán ser aceptados explícitamente por el CSI, previa justificación de la conveniencia de su aceptación.

Para los valores de riesgo residual que no sean aceptables se deberá elaborar el correspondiente Plan de Tratamiento que permita llevar los valores de riesgo a valores aceptables.

10. Datos de carácter general

La Compañía solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido.

De igual modo, adoptará las medidas de índole técnica y organizativa necesarias para el cumplimiento de la normativa de Protección de Datos, cumpliendo así con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), así como a la Ley Orgánica 3/2018, de Protección de Datos Personales y garantías de los derechos digitales (LOPDGDD).

A tal fin, la Compañía dispone de un manual de protección de datos y privacidad. El responsable es el Delegado de Protección de Datos y responsable del área de privacidad.

11. Desarrollo de la Política de Seguridad

Esta Política de Seguridad se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.

La documentación de políticas y normativas de seguridad, así como esta Política de Seguridad se encontrará a disposición de todo el personal de la Compañía que necesite conocerla y, en particular, el personal que utilice opere o administre los sistemas de información y comunicaciones o la información misma albergada en dichos sistemas o los servicios prestados por la Compañía.

12. Compromiso de la Dirección General

La Dirección General de la Compañía manifiesta su compromiso formal con el apoyo a los planes de seguridad que se deriven de la aplicación de esta Política. Dicho apoyo se concretará en:

- proporcionar los recursos humanos y económicos necesarios, dentro de las posibilidades presupuestarias;
- asignar roles y responsabilidades a las personas asociadas a los planes de seguridad;

- apoyar la formación de los recursos humanos implicados en los planes de seguridad para que adquieran el nivel de concienciación y las competencias necesarias;
- velar por el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información;
- facilitar las comunicaciones con otras organizaciones en materia de Seguridad de la Información;
- promover la mejora continua en el ámbito de Seguridad de la Información.

El compromiso con el apoyo a los planes se manifiesta con la aprobación del presente documento.

13. Estructura de la documentación de Seguridad

La documentación relacionada con la seguridad se evaluará en cuatro niveles de tal forma que cada documento de un nivel se base en el del nivel superior.

Los niveles de documentación que se establecen son:

- **Primer nivel: Política de Seguridad**
  - De obligado cumplimiento.
  - Aprobado por el CSI.
- **Segundo nivel: Políticas y/o Normativas de seguridad TIC**
  - De obligado cumplimiento, según el alcance organizativo, técnico o jurídico de que se trate.
  - La responsabilidad de aprobación en este nivel será del Responsable de Seguridad bajo la supervisión del CSI.
- **Tercer nivel: Procedimientos de seguridad TIC**
  - Procedimientos técnicos orientados a dar cumplimiento a lo dispuesto en la Normativa de seguridad TIC.
  - La responsabilidad de aprobación en este nivel será del Responsable del Sistema bajo la supervisión del Responsable de Seguridad.
- **Cuarto nivel: Informes TIC, registros y evidencias electrónicas.**
  - Informes TIC: Documentos de naturaleza técnica que recogen los resultados y conclusiones de un estudio o una evaluación.
  - Registros de actividad o alertas de seguridad: Documentos técnicos que incluyen amenazas y vulnerabilidades de los sistemas de información y comportamientos de los usuarios
  - Evidencias electrónicas: Generadas en cualquier momento durante el ciclo de vida del sistema de información.
  - La responsabilidad de la existencia de tales documentos es del Responsable del Sistema.

14. Publicación de la Política de Seguridad

El presente documento se publicará, de modo que esté accesible por todos los empleados y las partes interesadas de la Compañía.

15. Revisión y aprobación

La Política de Seguridad de la Información será revisada, al menos, cada TRES años.

La presente Política de Seguridad de la Información ha sido aprobada por la Dirección y será aplicable a partir del día siguiente al de su publicación.

Se firma por

Fdo: ANTONIO VICENTE CONTRERAS CEO

Fecha: 24-07-2024

| **ISOTADER CALIDAD, S.L.** | info@isotader.com | www.isotader.com |

| +34 968 900 300 | **MURCIA**, Edificio CEEIM, M6, 30100, Espinardo, **SPAIN** |